

**REMARKS****Claim and Application Status**

Claims 9-29 are pending in the present application.

Claims 1-8 have been cancelled without prejudice to prosecuting these claims in a related application. Claims 23 and 28 have been amended as suggested by the Examiner to address minor typographical issues.

Paragraphs 1 and 2 have been amended to now include publication numbers for the related applications. And paragraphs 26 and 43 have been amended to address minor typographical issues.

Applicants submit that no new matter has been added.

**Art-based Rejections**

Claims 9-14 stand rejected as being anticipated by assignee's US Patent No. 6,505,160 B1 (Levy).

Claims 15-29 stand rejected as being anticipated by US Patent No. 6,332,193 B1 (Glass).

Applicants respectfully traverse these rejections.

***Claim 9 in view of Levy***

The Office cites Levy at Col. 15, lines 55-62 as teaching *associating a second image in a database with a first identifier* as recited in claim 9. Yet we understand the cited Levy passage to deal with a transmarking process, which, e.g., may leave an existing embedded identifier in tact and layer an additional identifier onto a media object. The transmarking process may alternatively include, e.g., adding an additional or new identifier tag to headers or footer in a file format.

Respectfully, this passage is not understood to teach *associating a second image in a database with a first identifier*, in combination with the remaining features of claim 9. (Remember, claim 9 relates to a method to manage images, where the images include a first image having a first identifier steganographically embedded in the first image in the form of a digital watermark. The first image is retrieved from a database, is altered to create a second image; and a second identifier is steganographically embedded in the second image in the form of a digital watermark. The second image is associated in the database with the first identifier.)

Withdrawal of the rejection is respectfully requested.

*Claim 15 in view of Glass*

Glass discusses a method and apparatus for collecting and securely transmitting biometric data (e.g., an iris image) over a network. It appears that the biometric data is used to regulate access to a secured resource like a bank account.

Glass recognizes that an image (e.g., an iris image) will be fraudulently accessed or intercepted (see, e.g., Col. 1, lines 60-67; and Col. 2, lines 13-14). Thus, Glass tries to secure biometric image data in such a manner that undetectable substitution or tampering of the image data prior to biometric template conversion is difficult to perform (see, e.g., Col. 2, lines 58-61).

To help authenticate an image, a digital signature (a hash function – see Col. 6, lines 40-45) can be directly embedded in a biometric image (see, e.g., col. 7, lines 7-9).

Glass envisions that an embedded image will be fraudulently accessed, despite including the embedded digital signature. Thus, in the bank account example at Col. 9, a server checks to see if the image has been accessed and tampered with before allowing access to the requester's bank account, see, e.g., Col. 9, lines 37-42; lines 51-52; and lines 54-56. (The authentication server 10, which includes the bank account (i.e., secured

resource 17 in FIG. 7), itself accesses the image to determine whether the image has been tampered with, see, e.g., image authentication module 15, and col. 9, lines 40-50.)

While Glass may try to regulate access to a bank account based on evaluating a biometric image, Glass is not understood to teach or suggest: comparing a first image security level with a user security level; and allowing access to the first image based on a result of the comparison step, in combination with the remaining features of claim 15.

We respectfully submit that claim 15 should be allowed.

*Claim 23 in view of Glass*

In an analogous manner, Glass is not understood to teach or suggest a gatekeeper to regulate the flow of at least a first image between a first user terminal and a second user terminal, where the first image includes at least a first digital watermark including a first identifier, and where the gatekeeper determines a security level associated with the first image, compares the first image security level with a user security level, *and allows access by the second user terminal to the first image based on a result of the comparison*, in combination with the remaining features of claim 23.

Claim 23 should be allowed.

*Claim 28 in view of Glass*

In an analogous manner, Glass is not understood to teach or suggest means for comparing a first image security level with a user security level; and means for allowing access to the first image based on a result of said comparing means, in combination with the remaining features of claim 28.

Claim 28 should be allowed.

*Dependent Claims*

The dependent claims are believed patentable in their own right, in addition to being patentable based on their respective independent claims.

Favorable consideration is requested.

Information Disclosure Statement

Applicants are planning to submit an Information Disclosure Statement and Form 1449 for consideration by the Office. The Examiner is respectfully invited to contact the undersigned if the IDS has not been matched with the file by the time the Examiner picks up this Amendment for consideration.

Conclusion

The application is believed to be in condition for allowance. An early notice of allowance is respectfully requested. (Applicants need not belabor the other shortcomings of the art at this time.).

Nevertheless, the Examiner is invited to telephone the undersigned at 503-495-4575 if any issue remains.

Date: July 28, 2003



23735

PATENT TRADEMARK OFFICE

Phone: 503-885-9699

FAX: 503-885-9880

Respectfully submitted,

DIGIMARC CORPORATION

By St SL

Steven W. Stewart

Registration No. 45,133